12-06-99 /A

Case Docket No. PHA 23,637

THE COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

Enclosed for filing is the patent application of Inventor(s):
MICHAEL EPSTEIN

For: KEY DISTRIBUTION VIA A MEMORY DEVICE

ENCLOSED ARE:
[X] Associate Power of Attorney;
[X] Information Disclosure Statement, Form PTO-1449 and copies of documents listed therein;
[ ] Preliminary Amendment;
[X] Specification (16 Pages of Specification, Claims, & Abstract);
[X] Declaration and Power of Attorney:
     (2 Pages of a [X] fully executed [ ] unsigned Declaration);
[X] Drawing (1 sheets of [ ] informal [X] formal sheets);
[ ] Certified copy of   application Serial No.   ;
[ ] Other: ;
[X] Assignment to PHILIPS ELECTRONICS NORTH AMERICA CORPORATION.

FEE COMPUTATION

CLAIMS AS FILED				
FOR	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE - 760.00
Total Claims	20 - 20 =	0	X $18 =	
Independent Claims	5 - 3 =	2	X $78 =	156.00
Multiple Dependent Claims, if any			$260 =	
TOTAL FILING FEE			=	$916.00

Please charge Deposit Account No. 14-1270 in the amount of the total filing fee indicated above, plus any deficiencies. The Commissioner is also hereby authorized to charge any other fees which may be required, except the issue fee, or credit any overpayment to Account No. 14-1270.
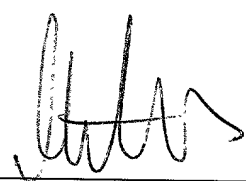
[ ] Amend the specification by inserting before the first line the sentence: --This is a continuation-in-part of application Serial No.   , filed   .--.

Daniel J. Piotrowski, Reg. 42,079
Attorney
(914) 333-9624
U.S. Philips Corporation
580 White Plains Road
Tarrytown, New York 10591
S:\pw\mo24PWQO.CNO

Key Distribution via a Memory Device

This application claims the benefit of U.S. Provisional Application No. 60/126,169, filed 03/25/99, Attorney Docket PHA 23,637P.

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of electronic security, and in particular to the encryption and decryption of copy-protected content material.

10

2. Description of Related Art

Digital recording techniques are commonly used to record copy-protected content material, such as audio and video recordings. Subsequent digital copies of such digital recordings are virtually indistinguishable from the original, and offer the same quality as the original.

15   As the ease of illicitly providing high-quality reproductions of copy-protected content material increases, the need for preventing such reproductions increases. At the same time, however, a legitimate purchaser of such copy-protected content material expects to be able to make copies of the content material for his or her own use. A number of "policy groups", such as the SDMI (Secure Digital Music Initiative), and others, have been formed in an attempt to reach

20   an equitable compromise between the opposing needs of the owners or vendors of the copy-protected material and the purchasers of copies of the copy-protected material. As a result of the actions of these policy groups, a variety of encryption and decryption techniques have been developed, and continue to be developed, to limit the number of times that a copy of copy-protected content material can be made, or to limit the number of times that a copy may be

25   played-back, or to place an expiration time on a copy. Similarly, encryption and decryption techniques have been developed that limit the type of actions than can be applied to the copy. For example, a copy may have a limit to the number of times that it can be copied, independent of the number of times that it can be played-back. A "copy-once, play-always" authorization would allow for an infinite number of play-backs, but only one copy; a "copy-never, play-10"

authorization would allow for ten play-backs, and no copies of this copy. For ease of reference, the term "rendering" is used herein to identify either a recording function or a playback function. For example, a recorder renders the material to a recording medium, a CD-player renders the material to an audio system, a DVD-player renders the material to an audio-visual system, and so on. In addition to limiting the number and type of renderings, the device that provides the limited-use copy may also limit the number of limited-use copies of the copy-protected material that are simultaneously available at any given time. That is, for example, if the number of limited-use copies at any given time is limited to ten, the compliant recorder will not provide an eleventh copy until at least one of the first ten copies is "checked-in", and marked as being expired, if not already so marked.

In a typical embodiment of a limited-use copy, the copy contains a counter or ticket that stores, in a secure manner, an indication of the authorized rights, and a compliant playback device updates the counter with each rendering or each passage of time, as appropriate for the particular authorized right. In the typical embodiment, the device that provides the limited-use copy and the device that renders the material share a cryptographic key or set of keys that are used to prevent the rendering of the material on an illicit device, and to prevent a modification to the authorization parameters. Typically, the content material is encrypted using a symmetric key, and this key is communicated to the rendering device in an encrypted form, using an asymmetric public key that corresponds to a private key that is associated with the rendering device. In this manner, only the intended rendering device is able to decrypt the encrypted content material. This asymmetric public key is also used to encrypt the authorization rights associated with the encrypted content material.

By limiting the number of simultaneously authorized copies, a compliant provider of the copies cannot be efficiently utilized for an illicit mass production. By limiting the number of times that a copy of copy-protected material can be rendered, the resale value of such a limited-use copy is substantially reduced, thereby diminishing the incentive to illicitly reproduce and sell these copies. At the same time, the purchaser of the original copy of the content material is provided virtually unlimited reproduction rights. The burden on the user of re-recording the expired copies from the original purchased copy is viewed to be minimal, particularly if the number of times that

the copy can be rendered before expiring is reasonably high, the number of simultaneous copies is reasonably high, and the effort required for the re-recording is low. The use of an expiration time, in lieu of an expiration based on the number of renderings, can also be used to minimize the resale value of each copy, yet allow the purchaser substantially unlimited reproduction rights. A time-

5   based system based on real time (clock time), however, is not often effective for copy protection, because many illicit copies could be made in a relatively short amount of time, and, conversely, most purchasers would be dissatisfied with a time limit that was not related to whether the material was being rendered during that time. Typically, time-based systems are based on a duration of time that the material is actually rendered, rather than real (clock) time.

10   Another scenario for the use of time-limited or usage-limited copies of copy-protected material is for the legitimate vendors of the copy-protected material to sell time-limited or usage-limited copies directly, potentially at a lower cost than the above referenced copies that allow for unlimited reproductions. For example, a limited-use copy may be provided via a download from the Internet, or via a broadcast from a provider, such as a cable or satellite television program

15   provider, with an option to purchase an unlimited-use copy. Or, limited-use copies can be provided as rental items, such as a single-use rental of a video recording that does not require the return of the recording within a limited time period. These and other scenarios for the use of limited-use copies of copy-protected content material can be expected to become increasingly common.

20   One known method of overcoming a limited-use copy protection scheme is termed a "replay attack". In this method, a bit-for-bit copy is made of the limited-use copy while it contains its full allocation of authorized usage or time, and stored in an archive. Although this copy cannot typically be used in a non-compliant rendering device, because the material is stored in a secured form, this copy can be used, or replayed, on a compliant device by re-recording the

25   bit-by-bit copy of the maximum allocated copy back onto the recording medium. Thus, even though the resale value of a limited-use copy of content material will be lower than the value of an unlimited-use copy, a counterfeiter may choose to provide such illicit limited-use copies, because of the ease of creating the copies, and the ease of overcoming the limited-use copy protection scheme.

30

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to provide an encryption method that precludes a replay attack on a limited-use protection scheme. It is a further object of this invention to provide a recording medium having properties that preclude a replay attack. It is a further object of this invention to provide a system that provides limited-use copies of copy-protected material that precludes a replay attack.

These objects and others are achieved by providing an encryption system having a secure item that is substantially unique for each recording of a copy of copy-protected content material. A memory element is provided in the recording medium that is readable but not writeable by external devices, and whose content changes each time material is recorded onto the medium. In a preferred embodiment, the content of this memory element is used to form a unique encryption key that is used to encrypt the encryption key that is used to encrypt the content material. This unique encryption of the content encryption key is further encrypted using a public key that corresponds to a private key of the intended rendering device. Although the unique encryption key is determinable by reading and processing the content of the externally read-only memory element, the decryption of the content encryption key requires both the unique encryption key and the private key of the intended rendering device. Because the unique encryption key is based on a content value of the read-only memory element that is unique to each recording to the recording medium, a subsequent illicit re-recording of the original encrypted content material onto the recording medium (a replay attack) will not provide the same unique encryption key as the unique encryption key used to originally encrypt the content encryption key. Because the unique encryption key of the replay attack differs from the original unique encryption key used to encrypt the content encryption key, the rendering device will be unable to decrypt the content encryption key, and thereby will be unable to decrypt the content material, and the replay attack will fail.

BRIEF DESCRIPTION OF THE DRAWING

The invention is explained in further detail, and by way of example, with reference to the accompanying drawing wherein:

FIG. 1 illustrates an example block diagram of an encryption system that provides a copy of copy-protected material that precludes replay attacks in accordance with this invention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an example block diagram of an encryption system 100 that provides a copy of copy-protected material on a recording medium 300 that precludes replay attacks in accordance with this invention. The encryption system 100 includes a content provider 200, a recording medium 300, and a rendering device 400. The content provider 200 records encrypted content material and associated information to the recording medium 300, for rendering by the rendering device 400. Any of a variety of conventional recording techniques can be employed, depending upon the form and structure of the medium 300. For ease of understanding, the components utilized to write to and read from the medium 300 are not illustrated in the example block diagram of the content provider 200 and rendering device 400 in FIG. 1.

In accordance with this invention, the recording medium 300 includes a recording indicator 310 that contains a unique number U. A new number U is created each time encrypted content material 221 is stored to the memory area 320 of the medium 300. Any number of techniques may be used to facilitate the production of this unique number U. In a straightforward embodiment of a solid-state medium 300, the recording indicator 310 includes a counter that is incremented by a modifier 315 with each write access 299 to the memory 320. In a more complex embodiment, the modifier 315 includes a random number generator that provides a new random number to the recording indicator 310 with each write access 299 to the memory 320. Other techniques are also viable, such as the use of a data-time stamp, and others.

In a preferred embodiment of this invention, the recording indicator 310 is embodied in the "disk sector tag" commonly associated with sectors of memory in a computer memory device. Corresponding tags can be written to optical or magnetic disks via a secure disk drive analogously

to the case of computer memory. That is, as the encrypted content material 221 is written to each sector of the memory area 320, the modifier 315 changes the disk sector tag of each sector that is written to. One or more of these changed disk sector tags thereby form the unique number U. By associating the recording indicator 310 with specific sectors, writes to other sectors within the medium 300 will not affect the tags associated with the sectors used to form the memory block 320 for storing the encrypted content material 320. In this manner, memory write operations are distinguishable, even if the medium 300 is not physically segregated into discrete memory blocks 310, 320, 340, 350 as illustrated in FIG. 1.

It should be noted that the number U can be the collection of all tags in the entire memory thus creating a single key KU for the entire contents of the media. Alternatively the number U and corresponding key KU can be for a single "disk sector" so that each section of the media can be separately rewritten without affecting the other sections of the media.

To prevent a replay attack, the recording indicator 310 is configured to be externally readable, but not externally controllable. That is, at each occurrence of a write access to the memory 320, the content recording indicator 310 changes in a manner that is not externally controllable. In this manner, if the legitimate contents in the medium 300 are copied to an archive, and then subsequently re-recorded on the medium 300 from the archive, the recording indicator 310 will, via the modifier 315, contain a different value U' (not illustrated) in the recording indicator 310 than the value U that had been in the recording indicator 310 when the legitimate contents were stored in the medium 300. Note that this value U' in the recording indicator 310 will be different than the original value U, regardless of whether a total bit-by-bit copy of medium 300 is archived, including a copy of the original value U. That is, because the recording indicator 310 is not externally controllable, the original value U cannot be rewritten into the recording indicator 310. In this manner, because a copy of the original contents of the medium 300 can be distinguished from the original contents, by comparing the original value U with the copy-produced new value U', a replay attack can be prevented.

To facilitate this replay defense, the original value U must be reliably and securely communicated to the rendering device 400 that enforces this defense. Any number of techniques may be employed to securely communicate the original value U. For example (not illustrated), the

original value U could be "digitally signed" by content provider 200, and this digitally signed information stored in the medium 300. A compliant rendering device 400 will verify that the digitally signed information is authentic, and then compare the digitally signed original value U to the current value of the value U in the recording indicator 310. If the current value U matches the

5   digitally signed value U, the rendering device 400 is assured that the encrypted content material 321 from the memory 320 is the encrypted content material 221 that was originally stored in the memory 320. If the current value U does not match the digitally signed value U, the rendering device 400 recognizes the attempted replay attack, and precludes a rendering of the content material.

10   In a preferred embodiment, as illustrated in FIG. 1, the value U 311 is used by the content provider 200 to encrypt an item when the encrypted content material 221 is originally recorded, and the value U 312 is subsequently used by the rendering device 400 to decrypt the item. If the value U 311 changes between the time the encrypted content material 221 is originally recorded and the time the rendering device reads the current value U 312, the rendering device 400 will be

15   unable to properly decrypt the item that was encrypted based on the original value U 311. If, on the other hand, the value U 311 that is used by the content provider 200 is the same as the value U 312 that is used by the rendering device 400, the rendering device 400 will properly decrypt the item that was encrypted based on the value U 312. In the example of FIG. 1, the aforementioned item that is encrypted based on the value 311 is a content key 202 that is used to encrypt, and

20   subsequently decrypt the encrypted content material 221.

        In the example embodiment of FIG. 1, an encrypter 220 is illustrated for providing the encrypted content material $E_{KC}(CM)$ 221 based on the content key KC. A key generator 210 creates a key KU 212 from the value U 311, typically via a hashing function. In a preferred embodiment wherein the recording indicator 310 is embodied within the disk sector tag for each

25   written sector, the key generator 210 creates the key KU 212 by iteratively hashing the unique value in each disk sector tag corresponding to the encrypted content material memory 320, and optionally, as discussed below, the unique value in each disk sector tag corresponding to the rendering rights memory 350.

An encrypter 230 uses the key KU 212 to encrypt the content key KC 202 to provide an encrypted content key $E_{KU}(KC)$ 231. At the rendering device 400, this encrypted content key $E_{KU}(KC)$ is shown as reference item 431. A key generator 410, similar to key generator 210, is used to generate a key KU 412, based on the value U 312 in the recording indicator 310 at the time that the medium 300 is read by the rendering device 400. A decrypter 430 decrypts the encrypted content key $E_{KU}(KC)$ 431 using this key KU 412. If the value U 312 corresponds to the original value U 311 that was used in the encryption of the content key KC 202, the decrypter 430 will provide a content key KC 402 that matches the content key KC 202. A decrypter 420 uses the decrypted content key KC 402 to decrypt the encrypted content material $E_{KC}(CM)$ 321 from the memory 320 of the medium 300. If the value U 312 does not correspond to the original value U 311, the rendering device key KU 412 will not match the original key KU 212, the decrypted content key KC 402 will not match the original content key 202, and therefore the decrypted content material CM 401 will not match the original content material 201, and will be substantially unrenderable.

Also illustrated in the example embodiment of FIG. 1, the content provider 200 includes an optional encrypter 240 that further encrypts the encrypted content key $E_{KU}(KC)$ 231 using a public key KP 204 that is associated with the rendering device 400. In this manner, the encrypted content key $E_{KU}(KC)$ 231 cannot be decrypted by a device other than the intended receiving device 400, thereby preventing a rendering of the content material 201 by other devices. This doubly encrypted key $E_{KP}(E_{KU}(KC))$ 241 is in a memory 340 of the medium 300. The corresponding rendering device 400 contains a decrypter 440 that decrypts the doubly encrypted key $E_{KP}(E_{KU}(KC))$ 341 from the memory 340 using a private key Kp 404 corresponding to the public key KP 204 of a public-private key pair. This decrypter 440 provides the aforementioned encrypted content key $E_{KU}(KC)$ 431.

For completeness, FIG. 1 illustrates an authorization module 450 in the rendering device 400 that enforces the limited rendering rights discussed in the Background of the Invention, above. Copending U.S. patent application, "Usage Dependent Ticket to Protect Copy-protected Material", U.S. serial number _____, filed _____ for Michael Epstein, Attorney Docket PHA _____ (Disclosure 700657), presents a method and system for allocating and

enforcing limited rights to each copy of encrypted content material that is stored on a recording medium, and is incorporated by reference herein. As applied to this invention, the content provider 200 includes a rights allocator 250 that stores allocated rights 251 on the recording medium 300. These allocated rights 251 are based on a usage parameter 352 of the medium 300

5 at the time that the encrypted content material 221 is recorded to the medium 300. The rights 251 may be encoded, for example, as a ticket that is "punched" by a modifier 355 each time the medium is accessed 499 by a rendering device 400, or as a counter that is decremented, and so on. In accordance with another aspect of this invention, the recording indicator 310 may be configured to change its stored value U whenever the memory area 350 that contains the rights

10 are written to from an external source, such as the content provider 200, or by an illicit attempt to modify the rights stored by the content provider 200. As discussed above, if the retrieved value U 312 differs from the original value U 311, the decrypted content material 401 will not match the original content material 201, and will be virtually unrenderable. If the rights in the memory 350 and the encrypted content material in the memory 320 have not been externally changed, the

15 decrypted content material 401 will match the original content material 201 and will be renderable. An authorization module 450 prevents the rendering 401', however, if the usage 353 of the medium 300 has exceeded the rights 351 allocated to the medium 300, via the gate 490. The rendering module 480 represents the components that render the decrypted content material 401, such as an audio system, an audio-video system, a computer system, and the like. The gate

20 490 represents any of a variety of means commonly available for inhibiting the production of the rendered material 401' from the content material 401 by the authorization module 450.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within

25 the spirit and scope of the following claims.

CLAIMS

I claim:

1. A recording medium comprising:

a first memory that is configured to store encrypted content material via a first write

operation,

a recording indicator that is configured to contain a unique identifier at each occurrence of

the first write operation, and

a second memory that is configured to store, via a second write operation, a secure item

based on the unique identifier when the encrypted content material is stored.

2. The recording medium of claim 1, wherein

the secure item includes an encrypted key that facilitates a decryption of the encrypted

content material, the encrypted key being dependent upon the unique identifier.

3. The recording medium of claim 1, wherein

the recording indicator includes a counter that is configured to be incremented by a

recording device when the recording device records the encrypted content material.

4. A rendering device that is configured to render content material corresponding to encrypted content material that is contained on a recording medium, the recording medium also including a recording indicator that contains an original value, the rendering device comprising:

one or more decrypters that are configured to decrypt the encrypted content material based on a current value of the recording indicator, such that the one or more decrypters provide the content material only when the current value of the recording indicator corresponds to the original value of the recording indicator, and

a renderer that is configured to render the content material.

5. The rendering device of claim 4, further including:

an authorization device that is configured to control the renderer based on a usage-measure associated with the recording medium and a validity period associated with the content material.

6. The rendering device of claim 4, further including

a key generator that creates a unique key based on the current value of the recording indicator, and

wherein

the one or more decrypters are configured to decrypt the encrypted content material based on the unique key that is based on the current value of the recording indicator.

7. The rendering device of claim 6, wherein

the one or more decrypters include:

a first decrypter that decrypts a doubly encrypted content key based on a private key of the rendering device to provide a singly encrypted content key,

5   a second decrypter that decrypts the singly encrypted content key based on the unique key that is based on the current value of the recording indicator to provide a content key, and

a third decrypter that decrypts the encrypted content material based on the content key to provide the content material.

10

8. A provider of content material comprising

a recorder that is configured to record encrypted content material and a corresponding

15   secure item on a recording medium,

the encrypted content material being encrypted based on a content key, and

the secure item being based on a value of a recording indicator of the recording medium when the encrypted content material is recorded on the recording medium.

20   9. The provider of claim 8, further comprising

an allocator that is configured to allocate rendering rights associated with the encrypted content material, and

wherein

the recorder is further configured to record the rendering rights on the recording medium.

25

10. The provider as claimed in claim 8, wherein

the secure item corresponds to an encryption of the content key based on the value of the recording indicator.

11. The provider as claimed in claim 8, further comprising

one or more encrypters that are configured to provide the secure item.

12. The provider of claim 8, further including

5   a key generator that generates a unique key based on the value of the recording indicator,
and

one or more encrypters that are configured to encrypt the content key based on the unique

key to produce the secure item.

10   13. The provider of claim 8, further comprising

a first encrypter that encrypts the content key based on a unique key that is dependent

upon a value of the recording indicator to produce a singly encrypted content key, and

a second encrypter that encrypts the singly encrypted content key based on a public key

that is associated with a rendering device to produce a doubly encrypted content key

15   corresponding to the secure item.

14. A method of providing content material, the method comprising:

    recording encrypted content material on a recording medium, the encrypted content material being dependent upon the content material and a content key, and

    recording a secure item on the recording medium, the secure item being dependent upon a

5 recording indicator that is associated with the recording medium.

15. The method of claim 14, further including

    recording rendering rights associated with the encrypted content material on the recording medium.

10

16. The method of claim 14, further including:

    generating a unique key that is based on the recording indicator,

    encrypting the content key using the unique key to produce the secure item.

15 17. The method of claim 14, wherein

    the method further including:

        generating a unique key that is based on the recording indicator,

        encrypting the content key using the unique key to produce a singly encrypted content key, and

20   encrypting the singly encrypted content key using a public key associated with a rendering device to produce the secure item.

18. A method of rendering content material from a recording medium that includes encrypted content material, an encrypted content key, and a recording indicator, the method comprising:

determining a unique key based on the recording indicator,

decrypting the encrypted content key based on the unique key to provide a content key,

5   decrypting the encrypted content material based on the content key to provide the content material, and

rendering the content material.

19. The method of claim 18, wherein

10   the recording medium also includes rendering rights, and

rendering the content material is dependent upon the rendering rights.

20. The method of claim 18, wherein

decrypting the encrypted content key includes:

15   decrypting the encrypted content key based on a private key to provide a singly encrypted content key, and

decrypting the singly encrypted content key based on the unique key to provide the content key.

20

Key Distribution via a Memory Device

ABSTRACT OF THE DISCLOSURE

5   An encryption system prevents a replay attack by providing a secure item that is substantially unique for each recording of copy-protected content material. A memory element is provided in the recording medium that is readable but not writeable by external devices, and whose content changes each time select material is recorded onto the medium. In a preferred embodiment, the content of this memory element is used to form a unique encryption key that is

10   used to encrypt the content encryption key. This unique encryption of the content encryption key is further encrypted using a public key that corresponds to a private key of the intended rendering device. Although the unique encryption key is determinable by reading and processing the content of the externally read-only memory element, the decryption of the content encryption key requires both the unique encryption key and the private key of the intended rendering device. Because the

15   unique encryption key is based on a content value of the read-only memory element that is unique to each recording to the recording medium, a subsequent illicit re-recording of the original encrypted content material onto the recording medium (a replay attack) will not provide the same unique encryption key as the unique encryption key used to originally encrypt the content encryption key. Because the unique encryption key of the replay attack differs from the original

20   unique encryption key used to encrypt the content encryption key, the rendering device will be unable to decrypt the content encryption key, and thereby will be unable to decrypt the content material, and the replay attack will fail.
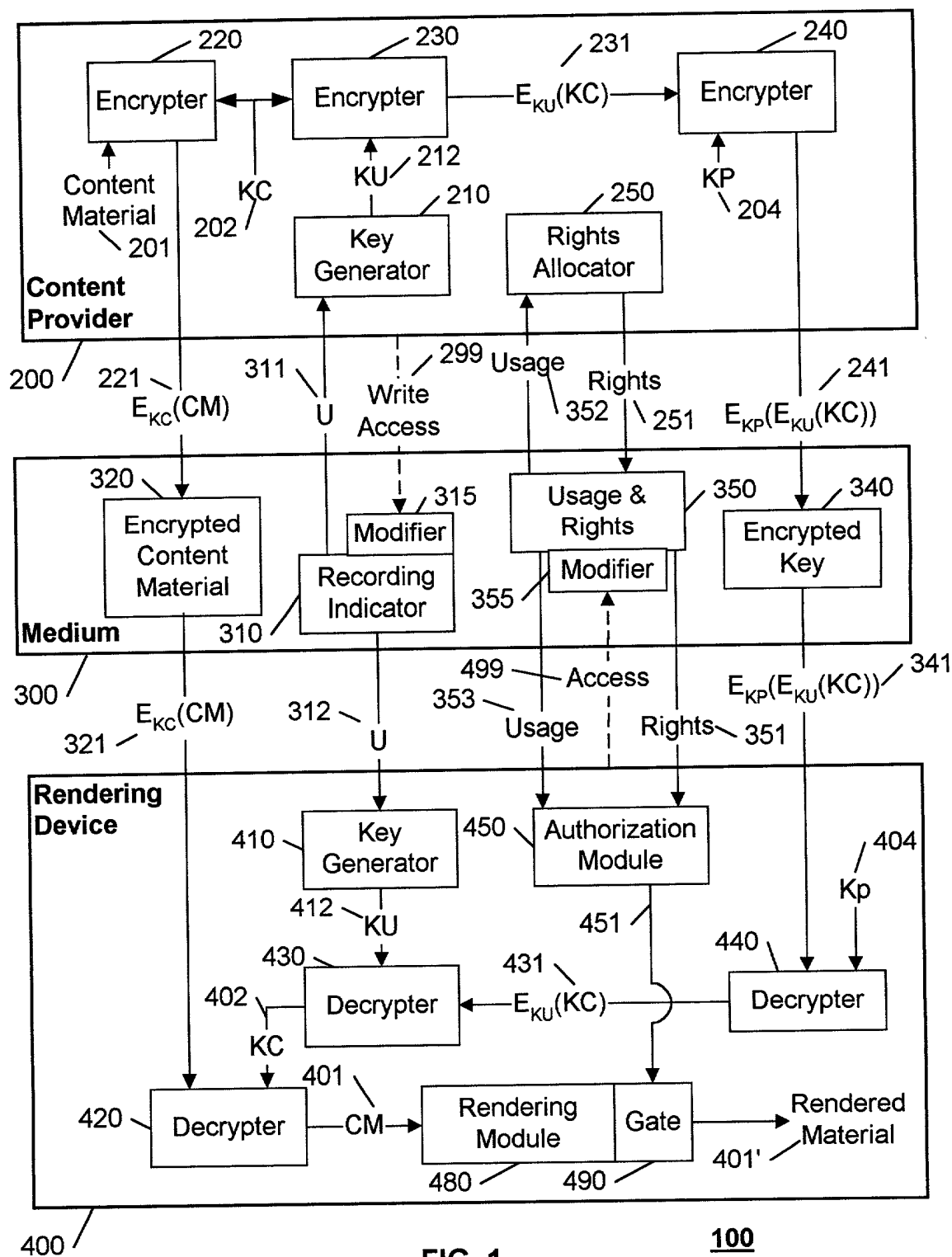
25

Content Provider

220 Encrypter

230 Encrypter

231 $E_{KU}(KC)$

240 Encrypter

Content Material
201

KC
202

KU 212

210 Key Generator

250 Rights Allocator

KP
204

200

Medium

221 $E_{KC}(CM)$

311 U

299 Write Access

Usage

Rights 352 \ 251

241 $E_{KP}(E_{KU}(KC))$

320 Encrypted Content Material

315 Modifier

350 Usage & Rights

340 Encrypted Key

Recording Indicator

355 Modifier

310

300

321 $E_{KC}(CM)$

312 U

499 Access

353 Usage

Rights 351

341 $E_{KP}(E_{KU}(KC))$

Rendering Device

410 Key Generator

450 Authorization Module

404 Kp

412 KU

451

440 Decrypter

430 Decrypter

402 KC

431 $E_{KU}(KC)$

401

420 Decrypter

CM

480 Rendering Module

490 Gate

Rendered Material

401'

400

FIG. 1

100

DECLARATION and POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **Key Distribution Via a Memory Device**

the specification of which (check one)

_X_ is attached hereto.

___ was filed on _____ as Application Serial No. _____ and was amended on _____

_____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, ∍1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, ∍ 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, ∍120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, ∍112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, ∍1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PRIOR UNITED STATES APPLICATION(S)

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)
60/126,169	March 25, 1999	Pending

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

SEND CORRESPONDENCE TO: Corporate Patent Counsel; U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591	DIRECT TELEPHONE CALLS TO: Daniel J. Piotrowski (914) 333-9624

Dated: 11/29/99	Inventor's Signature: _[signature]_		
Full Name of Inventor	**Last Name:** Epstein	**First Name :** Michael	**Middle Name:** A.
Residence & Citizenship	**City** Spring Valley	**State or Foreign Country** New York	**Country of Citizenship** United States of America
Post Office Address	**Street** 16 Dorset Road	**City** Spring Valley	**State or Country** New York	**Zip Code** 10977

Dated:	Inventor's Signature:		
Full Name of Inventor	**Last Name:**	**First Name :**	**Middle Name:**
Residence & Citizenship	**City**	**State or Foreign Country**	**Country of Citizenship**
Post Office Address	**Street**	**City**	**State or Country**	**Zip Code**

Dated:	Inventor's Signature:		
Full Name of Inventor	**Last Name:**	**First Name :**	**Middle Name:**
Residence & Citizenship	**City**	**State or Foreign Country**	**Country of Citizenship**
Post Office Address	**Street**	**City**	**State or Country**	**Zip Code**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

MICHAEL EPSTEIN

Serial No.

Filed: CONCURRENTLY

KEY DISTRIBUTION VIA A MEMORY DEVICE

Atty. Docket

PHA 23,637

Group Art Unit:

Examiner:

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

APPOINTMENT OF ASSOCIATES

Sir:

     The undersigned Attorney of Record hereby revokes all
prior appointments (if any) of Associate Attorney(s) or Agent(s) in
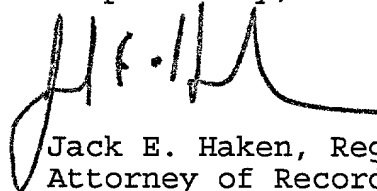the above-captioned case and appoints:

DANIEL J. PIOTROWSKI   **(Registration No. 42,079)**
c/o U.S. PHILIPS CORPORATION, Intellectual Property Department, 580
White Plains Road, Tarrytown, New York 10591, his Associate
Attorney(s)/Agent(s) with all the usual powers to prosecute the
above-identified application and any division or continuation
thereof, to make alterations and amendments therein, and to
transact all business in the Patent and Trademark Office connected
therewith.

     ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE
LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED
ATTORNEY OF RECORD.

Respectfully,

Jack E. Haken, Reg. 26,902
Attorney of Record

Dated at Tarrytown, New York
this 24TH day of NOVEMBER, 1999
S:\PW\MO23PWOO.CN0